ATTACHMENT NO. 3 – SUMMARY OF BRITISH STANDARD 7799 – 1:1999

Security Policy

Top management should set a clear direction and demonstrate their support for and commitment to information security through the issuance of an Information Security Policy effective across the organization. (3.1)

Security Organization

The objective of the information security infrastructure is to manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Responsibilities for the protection of individual assets and for carrying out specific security processes should be explicitly defined. (4.1 and 4.1.3)

Asset Classification and Control

The objective of assigning accountability for information assets is to maintain appropriate protection of organizational assets. All major information assets should be accounted for and have a nominated owner. Inventories should be maintained of all major information assets. (5.1)

Personnel Security

The objective of personnel security is to reduce the risks of human error, theft, fraud or misuse of facilities. Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment. (6.1)

Physical and Environmental Security

The objective of physical and environmental security is to prevent unauthorized access, damage and interference to IT services. IT facilities supporting critical or sensitive business activities should be physically protected from security threats and environmental hazards. (7.1)

Computer and Network Management

The objective of network and data center management controls is to ensure the correct and secure operation of computer and network facilities. Responsibilities and procedures for the management and operation of all computers and networks should be established. (8.1 and 8.5)

System Access Control

Access to computer services and data should be controlled on the basis of business services including computer systems, network services, applications and data. To detect unauthorized users or activities, systems should be monitored. (9.1, 9.2 and 9.7)

Systems Development and Maintenance

Security requirements should be identified and agreed prior to the development of IT systems to ensure that security is built into IT systems. (10.1)

Business Continuity Planning

Business continuity plans should be available to protect critical business processes from the effects of major failures or disasters. (11.1)

Compliance

The objective of security monitoring is to ensure compliance with organizational security policies and standards, and applicable laws. The security of IT systems should be regularly reviewed. (12.2)